International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Overview of Constraints and Diverse Attacks in Mobile Ad-hoc Networks

Srinivas Aluvala*[1], K. Rajasekhar[2]

Submitted: 26/08/2023 **Revised**: 12/10/2023 **Accepted**: 25/10/2023

Abstract: The task of relying on Mobile Ad hoc Networks (MANETs) is of significant importance due to the absence of a centralized framework. The continuous occurrence of clean nodules and the departure of aged ones in the MANET implementation necessitates the need to maintain records and provide appropriate authorization for new arriving nodes as well as existing nodes in the network. However, due to the presence of many types of breach threats and attacks, it becomes challenging to thoroughly examine any new node. Therefore, in order to ensure that only secure nodes are allowed to connect with the existing secure system. In a large cluster, the nodes within it are expected to engage in interactions, thereby facilitating or inhibiting access or communication between the vulnerable nodes or the trusted design. This dynamic system ensures the preservation of a stable, acquired, and reliable collection of transferable nodules. This paper provides a comprehensive examination of the limitations and diverse array of attacks in MANETs.

Keywords: *MANETs, limitations, threats, attacks and authorization.*

1. Introduction

A Mobile Ad hoc Network refers to a decentralized network configuration wherein the systems or devices establish connections with each other using wireless means, without relying on a central access point. Each mobile device within a network operates autonomously. Mobile phones have the ability to move freely and operate alone. The nodes inside the MANETs are responsible for the allocation of wireless resources, while the network's topology undergoes frequent and unpredictable changes. In MANETs, the fragmentation of communication links occurs frequently due to the unrestricted mobility of nodes. The density of nodules and nodes is contingent upon the specific applications employed by the organization in the context of MANETs. The advent of MANET has prompted in the development of several applications, including tactical systems, wireless sensor networks, data networks, device networks, and others. In addition to a multitude of therapies, there persist some stylistic concerns and challenges that must be addressed. The primary aim of mobile networking is to expand mobility in the area of autonomous and wireless domains, in which a set of nodes, can be routers and hosts, constitute the network devices in an adhoc fashion [2]. Numerous security vulnerabilities have been identified in wireless environments, particularly in the context of Mobile Ad hoc Networks. Additionally, a range of solutions have been developed to address these vulnerabilities. However, it should be noted that only a small subset of these providers offers a guarantee that is independent and capable of safeguarding critical issues. Considering these aspects, the primary objective of the mobile infrastructure less network is to ensure the consistent and dependable operation of wireless networks by integrating functions of routing into nodes in mobility. These systems are characterized by dynamic and often rapidly changing arbitrary multihop geographies, which are predominantly composed of bandwidth-constrained wireless networks.

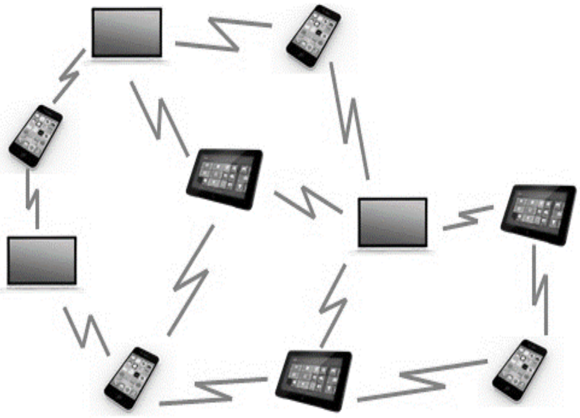

Fig 1: Mobile Ad-hoc Network

Mobile Ad hoc Networks exhibit a higher susceptibility compared to wired systems. This vulnerability arises from the presence of mobile phone nodes, the potential risks associated with compromised nodes inside the network, limited physical security measures, the dynamic state of the network topology, scalability challenges, and the absence of centralized administration [5]. As a consequence of these vulnerabilities, Mobile Ad hoc Networks exhibit a heightened susceptibility to malicious assaults.

Systems liveliness is the examination of accessibility,

[1] *Department of CSE, KL University, Guntur, India.*
Department of CS & AI, SR University, Warangal, India
ORCID ID: 0000-0002-9864-8184
[2] *Department of CSE, KL University, Guntur, India.*
ORCID ID: 0000-0003-4243-9700
** Corresponding Author Email: srinu.aluvala@gmail.com*

interdependence, and the stability of physical infrastructure of the network. Its examined in the early 1970s, namely the assessment of military command and also the communication units of the military. In the present-day scenario, there has been an increasing recognition of the significance of network survivability, driven by escalating need for mobile ad hoc networks. A vital factor in achieving reliable communication in Mobile Ad hoc Networks is the maintenance of network survivability. The survivability of the network facilitates the delivery of resilient services that sustain the network connectivity. The "functionality" refers to the capacity of a system to successfully complete its intended goal within a predetermined timeframe, even when faced with external threats, malfunctions, or failures. Nevertheless, the sustainability of a Mobile Ad hoc Network relies on the network's capacity to fulfil the survivability criteria [9]. The primary factor influencing the ability to survive within an ad hoc system is the system's capability to facilitate immediate communication between two nodes. The significance of connectivity within Mobile Ad hoc Networks (MANETs) arises from their inherent topology of self-organizing, where every node in the network act as both a router and terminal for transmitting packets to other nodes. The maintenance of connectivity poses a significant obstacle within the self-organizing framework of network geography, alongside the dynamic actions of nodes that often encounter failures in hyperlinks and nodes due to many variables such as interference, mobility, radio network effects, and battery constraints.

The primary aims of this Systematic Literature Review (SLR) in the present study are threefold: 1) to systematically assess the survivability structure of ad hoc systems [10], 2) to examine the design and metrics employed for the analysis of network survivability, and 3) to identify key unresolved issues in survivability modelling for the future research. This paper's work flow is as follows: Section 2 provides an overview of the assessment procedures. Section 3 of the study entails a comprehensive analysis of the ultimate results and the following assessment of these results within the framework of network survivability modelling. And further it explores the examination of survivorship measures and corresponding variables. In section 4 it provides a comprehensive analysis of various methodologies that can be employed to analyse the network model survivability. Section 5 gives thorough overview and conclusive analysis of the systematic literature review (SLR).

2. Classification of Manets Routing Protocols

Directing occupies a crucial role in network systems, for the transmission of data from one node to another. Ever since the introduction of commercial mobile ad hoc networks, the prominent factor in the field of directing is the analysis of concentration of the network. In order to meet the requirements of routing protocols that demonstrate correctness, speed, dependability, scalability, stability, fairness, robustness, Quality of Service (QoS) awareness, and energy efficiency of varied transmission protocols for Mobile Ad hoc Networks have been created. The aim of these protocols is to handle the challenges posed by highly dynamic network topologies in MANETs. They are designed to address the general limitations associated with dynamic nature of the system geography, which include increased power consumption, low transmission capacity and elevated error pricing. Numerous transmission protocols have been proposed for mobile ad-hoc networks over the years. In way to establish effective communication pathways amongst nodules, it is imperative to employ dependable routing protocols. There exists a variety of transmission protocols that are currently available for use in Mobile Ad hoc Networks. There exists a necessity for the establishment of a standardized approach in order to ascertain the availability of various methodologies [11]. The methods for steering Mobile Ad hoc Networks, as depicted in Figure 2-a, can be categorized into two broad approaches. The first approach is based on the mode of transmission, while the second approach is based on system architecture. Figure 2b categorizes the directing methods based on the routing approach. The methods used for directing can be classified as either table-steered or source-initiated. Figure 2(c) delineated the differentiation based on the network architecture, classifying them into conventional transmission, sequential routing, geographical (location-based routing), power-aware routing, and multicast transmission. In this article, our firm will is to discuss the routing procedure based on system architecture, since it has garnered significant attention and recognition from analysts and the industry.

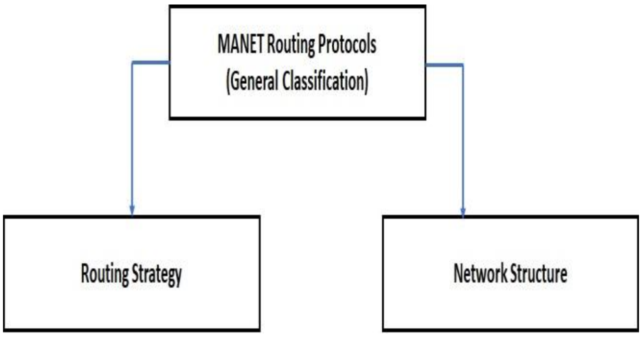

Fig 2a: Classification of Routing Protocols in MANETs

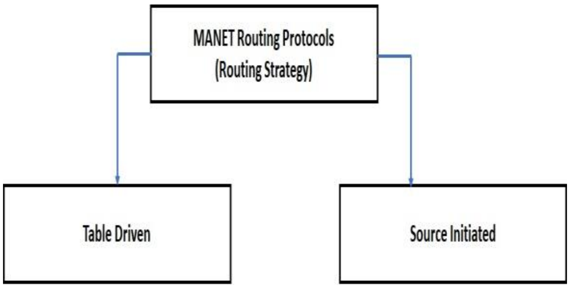

Fig 2b: MANETs Routing Protocols based on the routing strategy

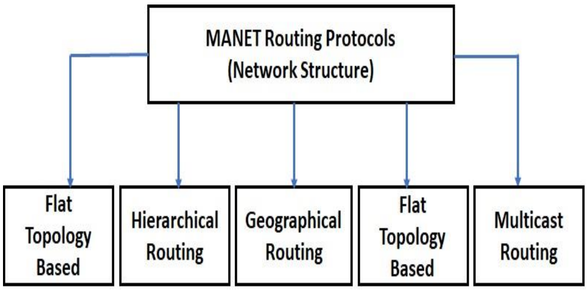

Fig 2c: MANETs Routing Protocols based on Network Structure

3. Flat Routing (Uniform) Or (Topology Based)

Geographic-based transmission methods utilize the pre-existing network topology and effectively handle the robust characteristics of Mobile Ad hoc Networks. Topology-based routing protocols have limited capability in comparison to geographical routing processes that leverage additional information to determine the location of nodes. Topology-based routing algorithms often require additional node geography information during the process of making routing decisions. Geography-based transmission can be further categorized as practical table-driven routing protocols, responsive on-demand routing strategies, and hybrid routing techniques. Figure 2 illustrates the comprehensive terminology associated with Flat Routing (Topology Based).

4. Manet Characteristics & Results

Mobile Ad hoc Networks exhibit unique attributes. Several aspects are described in the next section.

Decentralized architecture refers to a network structure where each individual node possesses the ability to freely assemble itself into a network [12]. Every node possesses the autonomy to make independent decisions on the forwarding or dropping of data packets during transmission. In summary, nodes have autonomous capabilities in terms of computation, switching, and communication. This particular type is referred to be decentralized since the nodes distributed throughout the system are not governed by a central authority.

Neighbor Discovery: In a Mobile Ad hoc Network, each node has the capability to identify its neighbouring nodes by transmitting wireless signals. The primary principle underlying the Mobile Ad hoc Network is the establishment of direct communication links between neighbouring nodes.

Heterogeneity: A Mobile Ad hoc Network might be comprised of nodes that exhibit diverse features. For example, it can establish an ad hoc network among the variety of devices like laptop, tablet, mobile phone, sensors, and iPod, similar to the formation of a network among multiple laptops.

The power source of all nodules in a Mobile Ad hoc Network is batteries. In a similar network, nodes with identical battery sizes are employed, whereas in a heterogeneous MANET, nodes with varying battery sizes are utilized. The reliable utilization of battery power for node functions, including as transmission, acquisition, and data processing, enables the conducting system to operate for extended durations.

The phenomenon of dynamically changing topology occurs when nodules autonomously prepare and assemble themselves while in motion, resulting in a continuously evolving geographic structure. Notwithstanding the ever-changing topology, the nodules exhibit a notable capacity for successful information transfer. The discovery of dynamical topological modifications and adaptability in MANETs was made by Yang et al. (2006), marking one of the earliest instances of such findings.

Seamless Interaction: A crucial need for the operation of Mobile Ad hoc Networks is the provision of uninterrupted communication among nodes once a link is established. Maintaining seamless communication between devices during node migration is indeed attainable.

The variability of cordless link capacity is a notable characteristic.

The multitude of declines resulting from environmental factors and degradation. The utilization of Orthogonal Frequency Division Multiplexing (OFDM) is employed at the physical layer of Mobile Ad hoc Networks.

Dispersed Operation: The absence of a backdrop network for the central control of system processes necessitates, dispersion of control among the nodes. In a Mobile Ad hoc Network, it is vital for the nodes to engage in cooperative behaviour and establish interactions among themselves. Each node assumes the role of a relay when necessary, facilitating the implementation of various functionalities such as routing and security measures.

Multi-hop routing refers to the process in which a node attempts to transmit data to other nodes that are beyond its immediate communication range. In order to accomplish this, the packet must be relayed through multiple intermediary nodes.

In a Mobile Ad hoc Network, each mobile node functions as both a host and a router, operating independently.

Lightweight Terminals: In most cases, the nodes in a Mobile Ad hoc Network (MANET) exhibit mobility and possess limited CPU capacity, low power storage, and tiny memory size.

The physical medium under consideration is the wireless interaction medium, which is capable of being deployed at many facilities with the requisite tools and ample resources. According to the available literature, it is possible that network access may not be subject to restrictions [2].

5. Manets Limitations

There is a current and anticipated demand for robust impromptu networking technologies. However, this social network technology, despite its remarkable adaptability, still faces certain limitations.

5.1. Throughput Drops with More Hops

Nodes that are located within the same transmission range has the capability to directly transmit data packets to one another. In the context of data transmission, it is important to note that when a node is required to transmit records to a non-neighbouring node, the data packages must be relayed through a series of intermediary nodes, effectively functioning as modems. This observation indicates a rise in the diversity of jumps executed. The increase in the number of jumps will lead to a rapid decrease in throughput. Node 2 may experience disruption in communication due to the presence of node 3, hence rendering it non-active. Consequently, as a result of the inclusion of supplementary hops, a larger number of vacant nodules persist, thereby reducing the overall throughput.

The decline in throughput is observed in conjunction with the escalation of mobility.

The presence of highly mobile nodes is likely to lead to increased costs due to frequent changes in network structure. The increase in the volume of transmitted package shipments can be attributed to the need for establishing alternative routes following disruptions in the existing transportation network. In practice, the routing table is utilized by each node to store a comprehensive record of all accessible destinations, together with the corresponding number of hops required to reach each destination. Enhancements in geographical factors will undoubtedly be evident in the directorial framework. All updates made to the transmitting table are disseminated to all other nodes in the network. This imposes a greater financial burden on the overall network. When the expenses are of a significant magnitude (13), a smaller proportion of the budget is allocated to the gear box of records, resulting in a decreased throughput.

5.2. Delay

The concept of delay is associated with the standard interval during which a package is in transit, spanning from its departure from the source to its arrival at the destination. As previously observed, it is necessary to provide continuous occupation of the nodes for both packet transmission and reception in order to enhance the network's throughput. As a result, it may be inferred that the queue of each node consistently remains occupied, leading to an extended period of delay.

The Mobile Ad hoc Network, with its inherent dynamism and adaptability, exhibits promising potential for military applications. The system possesses the capability to surpass conventional limitations of interactions by utilizing auto relaying and self-healing/forming components. When combined with the Airborne Communication Node (ACN) concept, Mobile Ad hoc Networks have the potential to provide the 3rd Generation Singapore Armed Forces (3G SAF) with extensive communication coverage and operational flexibility, particularly in low-tier planned environments. In addition to aiding for conventional duties of the SAF armed forces, Mobile Ad hoc Networks, due to their lack of infrastructure, can also be effectively utilized for increasingly important operations

such as Operations Other Than War (OOTWA), where the ease of deployment is a primary concern.

In the commercial domain, advancements in Mobile Ad hoc Networks continue to be ongoing. The integration of advanced technologies, such as Multiple- Input Multiple-Output (MIMO) and smart aerials, has the potential to enhance the connectivity experience within a Mobile Ad hoc Network. The process of trial and error is indeed crucial in identifying, implementing, and integrating technologies that can transform the SAF into a resilient 3G force.

6. Various Attacks in Manets

1. The black hole attack is an aggressive tactic whereby the aggressor seeks to infiltrate the multicast forwarding infrastructure, such as through the execution of a rushing assault, in order to disrupt the transmission of information packets within the multicast network. Subsequently, it fails to retain a significant portion or the all of the data packets it receives, instead of transmitting them to the subsequent node along the designated route. This particular type of incantation frequently results in a significantly low rate of package dissemination.

2. In the case of an assault by a next-door neighbor, when a packet is received, an intermediary node records its own identification within the packet before transmitting it to the subsequent node. The perpetrator surreptitiously forwarded the package without including any form of identification within the package. Generate a pair of nodules that are not

closely connected in the communication network, but are perceived as adjacent to one other (i.e., only one step away), resulting in a disturbed pathway.

3. The phenomenon of jellyfish aggression involves the initial intrusion of a jellyfish attacker into a multicast transmitting team. Subsequently, it exhibits an excessive delay in transmitting data packets for a certain duration prior to their onward transmission. This leads to significant delays in end-to-end communication, thereby compromising the efficiency of real-time applications.

4. Wormhole attack: A malicious actor captures packets at a certain location inside the system and subsequently transmits them to a different location. The process of directing can encounter challenges when the transmission of control information is tunneled. The passage connecting two collaborating individuals is commonly known as a wormhole. Wormhole attacks pose significant risks to the transmission methods employed in Mobile Ad hoc Networks.

7. Conclusion

This study aims to compare various security devices in order to evaluate their effectiveness in addressing system complexities. The majority of previous and contemporary systems have prioritized the provision of transmission services without adequately considering high-level surveillance and minimizing delays. The research study instructions will primarily focus on the capabilities of artificial neural networks (ANN) and the coordination function of surrounding nodes in order to address the challenges of secure communication and minimize problems in mobile phone unplanned networks. This study presents a comprehensive analysis of the limits and diverse attack strategies in Mobile Ad hoc Networks.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] AnjuRan, Sandeep Gupta, “Review on MANETs Characteristics, challenges, Application and Security Attacks”- International Journal of Science and Research (IJSR) 2015.

[2] Harmanpreet Kaur, P.S. Mann, “Detection of Black Hole Attack in Mobile AD HOC networks a survey” International Journal of Science and Research (IJSR) 2014.

[3] Aarti, Study of MANET: Characteristics, challenges,Application and Security Attacks- International Journal of Advance Research in Computer Science and software Engineering,2013.

[4] Z. Karakehayov, “Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks,” Workshop on Real-World Wireless Sensor Networks, June 20–21, 2005.

[5] Y-C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE SAC, Vol. 24, No. 2, Feb. 2006.

[6] HaoYang, Haiyun & Fan Ye ― Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.

[7] Buttyan, L., and Hubaux, J. P. Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications: Special Issue on Mobile Ad Hoc Networks, 8(5), 2003.

[8] S. Corson and J. Macker, “RFC 2501 - Mobile Ad Hoc Networking (MANET): Routing Protocol Pe”, Network Working Group, Request for Comments: 2501, University of Maryland, Naval Research Laboratory, JAN 1999.

[9] Srinivas Aluvala, K. Raja Sekar, Deepika Vodnala, “An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks”, Elsevier - Procedia Computer Science, 92, pp.554 – 561, 2016, DOI. 10.1016/j.procs.2016.07.382.

[10] Deepika Vodnala, Dr. S. Phani Kumar, Srinivas Aluvala “An Analysis Study of Various Multicasting Routing Protocols in MANETs”, International Journal of Emerging Technology and Advanced Engi- neering; Volume 4, Issue 8, August 2014, page(s) 424- 429, ISSN 2250- 2459, Impact Factor: 2.324.

[11] Srinivas Aluvala, K. Raja Sekar, Deepika Vodnala, "A Novel Technique for Node Authentication in Mobile Ad-hoc Networks" in Elsevier - Perspectives in Science, Volume 8, Issue 1, Page No(s) 680 - 682, SEP. 2016, [ISSN(Print):2213-0209], DOI:10.1016/j.pisc.2016.

[12] Srinivas Aluvala, G.Sunil, Nagendar Yamsani, Bura Vijaykumar “An Empirical Study of Issues in Security and Routing of Multicast Routing Protocols in Mobile Ad Hoc Networks” International Journal of Engineering and Technology (IJET), ISSN 2227-524X, Vol 7, No 3.34 (2018), special Issue 34, page(s): 1015–1018, December 2018, DOI. 10.14419/ijet.v7i3.34.25353.

[13] Srinivas Aluvala, K. Raja Sekar, Deepika Vodnala “Analysis of Security Threats and Issues in MANETs”, International Journal on Advanced Computer Theory and Engineering (IJACTE), ISSN (Print): 2319-2526, Volume 4, Issue 5, page(s): 23-28, 2015, Impact Factor: 1.64.